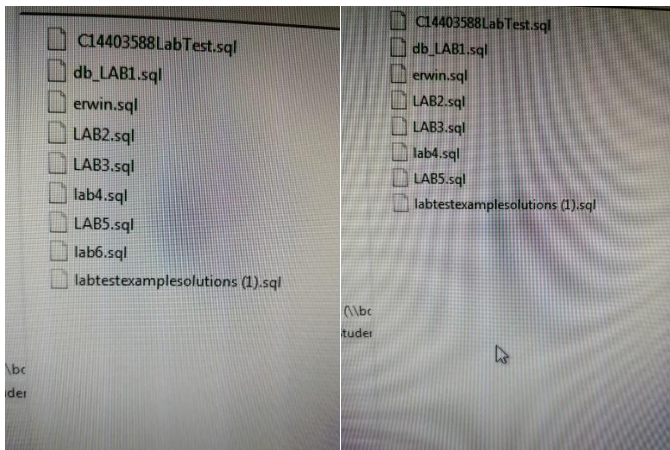
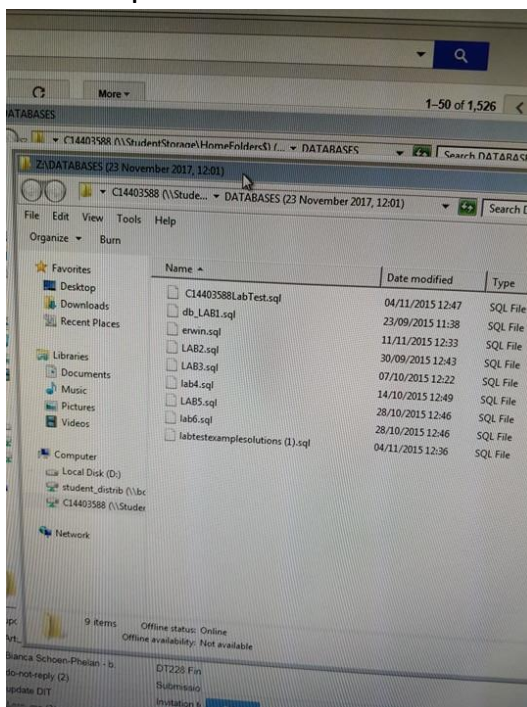


Forensics week 11 Lab

1. To recover files off a windows operating system the user can use the windows feature “previous versions” to look at the dates the files were edited. This allows the user to roll back to versions or recover files have been deleted completed. The file that was deleted was a .sql file. We can see by the pictures below this was deleted.



The pictures above show the lab6.sql file has been deleted. We then right click the folder that file was saved in and click the previous versions tab. This contains a set of dates and the files content on that date. We then pick the version we want and the file is back. We can see the file and the previous version below.



2. An employer's responsibility to securing information in the organisation is defined by the Data protection acts 1998 and 2003. This applies to every business that uses any form of data relating to customers or staff. The people who control and oversee the use of data are called data controllers. The data protection act follows 8 key principles. The first is that data must be processed fairly and lawfully. This means employees have to respect the privacy when processing data and remain in the parameters of the law. The company must only take information into the company for specific reasons and in a lawful way. If there is no reason for the company to have a specific piece of data, this can result in serious repercussions. The next key principle is that data must be adequate, relevant and not excessive. Do not take any data that is not needed or do not take too much data. The data relating to people should be accurate and up to date. People's information is constantly changing and updating so the business must make sure the information they have is correct. The data should not be held any longer than is necessary. If a customer changes bank the bank should not keep the information they currently have of the person. Any information that is processed by a business should be in accordance with the rights of the data subject. The company cannot breach these rights. The data must be protected in appropriate ways. Meaning your data must be safe and not accessible to unauthorized people. Your data must not be transferred outside the European Economic Area, unless that country also has as high of a data protection standard as us. These keys ensure the highest level of data protection for the customers of your company.

References:

<https://www.techdonut.co.uk/staff-and-it-training/your-it-policies/sample-data-protection-policy-template>